Title (en)

A method of detecting anomalies in a message exchange, corresponding computer program product, and data storage device therefor

Title (de)

Verfahren zur Detektion von Unregelmäßigkeiten beim Nachrichtenaustausch, zugehöriges Computerprogrammprodukt und Datenspeicherungsvorrichtung dafür

Title (fr)

Procédé de détection d'anomalies dans un échange de messages, programme informatique correspondant et dispositif de stockage de données correspondant

Publication

**EP 2369529 A1 20110928 (EN)**

Application

**EP 10305292 A 20100324**

Priority

EP 10305292 A 20100324

Abstract (en)

The invention concerns a method of detecting anomalies in a message exchange by means of a binary classifier, the method comprising the steps of receiving (101) a plurality of training messages, each training message tagged as either normal or anomalous, and, based on the training messages, building the binary classifier for a test message, wherein the training messages and the test message conform to a text-based protocol and wherein, in order to build the binary classifier, the method comprises the steps of transforming (102) each training message into a multi-dimensional vector of features spanning a feature space, each feature corresponding to a contiguous substring of the respective training message, constructing (103) a hyperplane in the feature space, and building (104) the binary classifier based on the hyperplane. The invention further concerns a computer program product and a device therefor.

IPC 8 full level

**G06N 7/00** (2006.01); **G06N 20/10** (2019.01); G06F 21/00 (2006.01)

CPC (source: EP US)

**G06N 20/00** (2018.12 - EP); **G06N 20/10** (2018.12 - EP US); **H04L 63/1416** (2013.01 - EP); H04L 65/1104 (2022.05 - EP)

Citation (applicant)

- "An Intrusion Detection Model", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, vol. SE-13, no. 2, February 1987 (1987-02-01), pages 222 - 232
- VICTORIA J. HODGE; JIM AUSTIN: "A Survey of Outlier Detection Methodologies", ARTIFICIAL INTELLIGENCE REVIEW, vol. 22, no. 2, October 2004 (2004-10-01), pages 85 - 126

Citation (search report)

- [XI] US 2007177607 A1 20070802 - NICCOLINI SAVERIO [DE], et al
- [I] EP 2112803 A1 20091028 - ALCATEL LUCENT [FR]
- [A] EP 2134057 A1 20091216 - ALCATEL LUCENT [FR]
- [XI] KONRAD RIECK ET AL: "A Self-learning System for Detection of Anomalous SIP Messages", 1 July 2008, PRINCIPLES, SYSTEMS AND APPLICATIONS OF IP TELECOMMUNICATIONS. SERVICES AND SECURITY FOR NEXT GENERATION NETWORKS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 90 - 106, ISBN: 978-3-540-89053-9, XP019109765
- [XI] "Self-Learning SIP Anomaly Detection Algorithm and Architecture (SIP Firewall) - Protecting SIP Networks From Attack", December 2008 (2008-12-01), XP002589096, Retrieved from the Internet <URL:http://innovationdays.alcatel-lucent.com/2008/documents/SIP%20Firewall.pdf> [retrieved on 20100628]
- [XI] MOHAMED NASSAR ET AL: "Monitoring SIP Traffic Using Support Vector Machines", 15 September 2008, RECENT ADVANCES IN INTRUSION DETECTION; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 311 - 330, ISBN: 978-3-540-87402-7, XP019105447
- [XI] JINGTAO YAO, SONGLUN ZHAO, AND LISA FAN: "An Enhanced Support Vector Machine Modelfor Intrusion Detection", vol. LNAI 4062, 27 September 2006 (2006-09-27), Lecture Notes in Computer Science, Springer-Verlag, pages 538 - 543, XP002589097, Retrieved from the Internet <URL:http://www.springerlink.com/content/545p551497h0p3u2/fulltext.pdf> [retrieved on 20100705]

Cited by

CN107025547A; CN108337216A; CN104899507A; CN108337217A; CN111740957A; CN110334083A; CN112036296A; CN111242272A; CN102499651A; CN109885030A; CN108431834A; CN108712404A; US10394687B2; WO2016085272A1; WO2016085273A1; US10609061B2; US10616253B2; US11165806B2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

Designated extension state (EPC)

AL BA ME RS

DOCDB simple family (publication)

**EP 2369529 A1 20110928**

DOCDB simple family (application)

**EP 10305292 A 20100324**